FEDLINE EFT CHAPTER 19

(FILE NAME ON DISK # 2 = S2C19.WPD)

This section is designed specifically to address the proper setup of terminal related security for the Federal Reserve Fedline terminals. It covers only the wire transfer function of Fedline. A number of other security and control issues surround the wire transfer function, including balancing functions, reviewing Fedline activity logs, separation of duties, credit limits, collected balances, transferee identification, etc. These items may be reviewed through reference to Chapter 18, Wholesale EFT.

LOCAL SECURITY ADMINISTRATOR

The Local Security Administrator (LSA) is responsible for setting up new users on the local Fedline system. The LSA also is responsible for setting the function levels of all users. The LSA is a powerful user and has the tools to bypass all security and effectively send a transfer with no supervision, if other compensating controls, such as prompt balancing and timely activity log review, are not in effect. Internal controls and proper separation of duties are important in protecting the bank from significant risk.

The LSA should be someone in the bank who has *NO* day-to-day operational duties on the Fedline terminal. The LSA's main purpose should be to add new users and change function security levels. Anytime the LSA uses the terminal, a member of the daily operations staff should be present to monitor his/her actions. If the Fedline terminal has a power on password, it should be implemented and the password restricted from the LSA. In addition, the LSA should not have a host access logon at the Federal Reserve host mainframe computer. This would prevent the LSA from logging onto the host mainframe and sending a transfer immediately. However, the LSA could queue the transfer (TQ status), and the next time a valid transfer exchange was made, the unauthorized transfer would be sent in that batch. However, this method increases the chances that an unauthorized transfer would be detected.

The LSA with unrestricted access could perform the following functions to bypass security:

- Add two new user IDs having enter and verify capability and enter a transfer.
- Change the verification rule to N, thus eliminating the verification requirement.
- Change the verification threshold dollar amount to $99,999,999.99, thus circumventing verification.

Accordingly, these functions must be controlled.

MISCELLANEOUS SECURITY SETTINGS

User ID suspended – Consecutive bad password retries – Specifies the maximum number of consecutive invalid sign-on attempts operators can make before the local user ID is suspended. This prevents an unauthorized person from trying to guess the password of a legitimate user by limiting the number of invalid password retries. The Federal Reserve Board's recommended setting is 3.

Users must periodically change their password every XX days – Specifies the maximum number of days operators can use their password before they must change it. The Federal Reserve Board's recommended setting is 30.

Verification rule – This rule sets the message verification requirement. This prevents the origination of unauthorized (fraudulent) messages. This rule should require that more than one person be involved with the processing of transfers. Three options are available, N, U, and E (see the description of the option settings below). The Federal Reserve Board's recommended setting is E, however U is acceptable. (Note: This rule will affect all the types of message transactions that require verification; such as funds transfer, large dollar check returns and TT&L.)

Options:

- *N – No restriction (Very high risk)* – This option allows the operator who entered and/or updated a message also to verify that same message. There is no dual control of any wire transfers if this option is chosen. For example, Mary enters a message. She also can update and verify that same message.

- *U – Verifying operator cannot be the last operator who updated the transfer*. This option prevents the last operator who entered or updated a transfer from verifying that same message. It would allow the original operator to verify the transfer if it was changed by a second operator. For example, Mary enters a transfer and Paul updates (changes) that same message. Paul cannot verify that same message, but Mary can.

- *E – Verifying operator cannot be operator who entered or updated the transfer*. This option prevents any operator who entered or updated a transfer from verifying that same transfer. For example, Mary enters a transfer and Paul updates that same transfer. Neither Mary nor Paul can verify that same message. Some other Fedline operator who has verify access must verify the transfer.

Override and release rule – This field is used to indicate the level of restrictions placed on overriding and/or releasing transfers. This potentially allows users to bypass verification. Only operators with the *supervisor function* access level have the ability to perform the Override & release function. The Federal Reserve Board's recommended setting is E, however U is acceptable.

- *N – No restriction on override or release* – Any operator with the supervisor function access level can override or release the verification of a transfer regardless of any previous processing performed with the exception of messages that have a status of TQ, MC, or CN.

- *U – Limited restriction on override or release* – The operator overriding or releasing the transfer cannot be the operator who last updated the message.

- *E – Full restriction* – The operator overriding or releasing the transfer cannot be the operator who updated or entered the message.

Timeout Intervals – This timeout parameter minimizes the amount of time that a terminal remains active if a user forgets to sign-off. It causes the system to revert to the Fedline Sign-on screen after a specified amount of time during which no keystrokes have been entered at the PC. The Federal Reserve Board's recommended setting is 10 minutes.

Cycle-Date rollover and Print-delete option – This option allows the bank to select the type of report to be printed to document the previous day's wires that were queued for transmission, but were not sent, before they are deleted from the Fedline system. The software ships with FULL as the default.

- *FULL* – Prints a full recap report of the previous days wire transfers before they are deleted by the cleanup cycle date mode change program.

- *SUMMARY* – Prints an abbreviated report of the previous days wire transfers before they are deleted by the cleanup cycle date mode change program.

USER/ACCESS REPORT EVALUATION

Staff member(s) assigned the Local Security Administrator (LSA) function should be restricted from the funds transfer (FT) application. LSAs should not have access to the FT application. If the FT application is listed, it may indicate that the LSA is involved in ongoing funds transfer activity.

Staff member(s) assigned the LSA function should be restricted from the Host Communications (HC) function. A staff member with HC access could log on to the Federal Reserve host mainframe and transmit the wire transfer. (Note: The staff member must have a host logon ID and security access on the Federal Reserve host mainframe to implement the wire transfer. There is no way to determine on-site at the bank if a user has host access. This only can be determined by calling the data security department of the Federal Reserve Bank. The listing or non-listing of the HC application under the user's ID is usually a good indicator of their host access ability. However, this method of determination is not conclusive since the LSA can use the *Master ID* to activate this application at any time.)

The Local Security Administrator (LSA) should be assigned *only* the Local Administration (LA) application. Since the LSA should not be involved in the daily ongoing operation of the Fedline terminal. There is no reason for them to have access privileges to any other available applications other than LA.

Staff members should have no more than one user ID. Staff members with more than one user ID can by-pass the verification requirement by signing on with the first ID to enter transactions and then signing on with the second ID to perform the verification.

No more than two staff members should be assigned as Local Security Administrators. Local Administrator access is very powerful and therefore its use should be limited as much as possible. The Federal Reserve guidelines suggest an Administrator and one backup Administrator. Depending on the size of the institution, the existence of more than two staff members with Local Administrator capabilities should be criticized.

No staff members should have the funds transfer (FT) Supervisor or Manager function. These functions have funds transfer access levels that provide the ability to bypass the verification requirement. These access levels should only be activated by the Local Security Administrator in unusual circumstances. The Local Security Administrator should monitor the actions performed using these access levels and then deactivate these levels when the action is complete. It is possible that the Supervisor function is needed in other applications such as *Startup/Shutdown Control*. However, it is not normally needed in the funds transfer application.

No staff members other than the Local Security Administrator should have the Local Administration (LA) application priviledge. Verify that the staff members who operate the Fedline on a daily ongoing basis do not have the LA privilege listed under their user ID on the *User/Access report.* The ** listing grants access to all applications listed on the menu except the LA function. Therefore, the ** could be appropriate depending on the circumstances. The LA function will be specifically listed if the user has access to this application and should be criticized accordingly.

VERIFICATION FIELDS

The update funds application attributes option allows the staff members with Manager function level or the LSA to set the verification fields for wire transfers.

Available options range from no verification of any field to required verification of every field. In between these two extremes, the Manager or LSA can select individual fields that would require second operator verification. Verification refers to fields which must be re-keyed by a second operator. If none of the fields have an X next to them, no re-keying is required by the second operator. However, a second operator will still have to provide a sight verification by calling up the transfer on the screen and reviewing it. The Federal Reserve Board recommends that, at a minimum, verification of the dollar field should be required, (i.e., marked with an X to indicate that a second operator will have to rekey in the dollar amount). Some banks might choose additional fields to verify, such as, account number, routing number, etc.

VERIFICATION THRESHOLD

The update funds application attributes option allows the staff members with Manager function level to set the verification threshold for wire transfers.

Available options range from no verification of any transfers required to verification of every transfer required. In between these two extremes, dollar-floor limits also are available.

Normally, a bank should set the verify threshold to $0.00 which requires verification of all transfers by a second operator. If the bank should decide to set the verification level at a higher amount, this amount should be approved by the Board of Directors and noted in the minutes. (Note: an amount of $99,999,999,999.99 in the verify threshold field indicates that the requirement for verification by a second operator has been turned off.)

GENERAL CONTROLS

Master password backup storage – There might be a situation where a local administration function needs to be performed, but there are no Local Security Administrators available. Therefore, the Master User ID password should be stored in a secure location and be available for the operating personnel should the need arise. The Master User ID password should be changed by the LSA after it is used by the operating personnel.

Fedline configuration diskette – The diskette is used by the bank in conjunction with the Federal Reserve in case everyone is locked out of the system. The Fedline configuration diskette should be securely stored.

PC power-on password – Many microcomputers have the ability to activate a power-on password feature. This feature forces the input of a password before the computer will activate. If the Fedline terminal has this feature available, it should be activated. The Local Security Administrator(s) should not have access to this password. This control will prevent an LSA from entering transfer requests when the terminal is not monitored by operating personnel.

DISASTER /CONTINGENCY

Recovering wire transfer operations in a disaster situation is an operational concern. Generally, unless the bank sends and receives many transfers, the telephone can be used as a backup method. The wire transfer personnel should know where the current backup code word list is stored. Wire transfer terminals are standard PCs with a Federal Reserve issued encryption board. Turnaround time for acquiring new equipment should be fairly rapid.

The bank should be queried as to what its contingency plans are in the event of an equipment failure (e.g., encryption device failure) or the loss of the Fedline terminal(s). The banks contingency plan should include keeping a backup copy of the current version of the Fedline software available on diskette and periodically making a static file backup of the Fedline (backup static files function in the miscellaneous support application) application that will copy all customized data used by the bank (e.g., frequent ABA's, User ID's, and recurring transfers).

FEDWIRE WIRE TRANSFER FUNCTIONS

The following reflect Fedwire functions along with a brief description.

Entry/Update

- Create a message – Enter a transfer.
- Derive a reversal – Reverse a previously received transfer.
- Export a message file – Copy selected funds transfers onto a diskette.
- Import a message file – Copy funds transfers created using another processing system into Fedline.
- Update a message – Change detail information in a transfer.

Verify/Transmit

- Group release – Change status of a group of transactions for immediate release.
- Release transfers for transmit – Change status of transfer marked "held" to release.
- Verify a message – Verify a previously entered transfer.

Asst. Supervisory functions

- Add recurring template – Create new template.
- Delete recurring template – Delete template.
- Update recurring template – Modify template.

Supervisory functions

- Group override – Change status of a group of messages held from transmission.
- Message status override – Allows the status of a transfer to be changed (by-passes any verification).
- Modify screen defaults – Allows you to modify default data of the create screens which are automatically inserted whenever you create a message.
- Re-send message – Allows you to resend a previously transmitted message that may have been lost by the receiver or rejected by the host.

Managerial functions

- Resync. host – resequence transfer ID appl seq# numbers on Fed main frame.
- Update key verify – select fields in transfer fields entry that must be verified.
- Update application – specify dollar amount attributes of outgoing transfers that require verification.